

Ransomware: What is Ransomware? Why is Ransomware Harmful? Best Practices You Can Implement to Avoid Ransomware Attacks

Susan Doucette

Director, Program Underwriting

February 16, 2022

Tokio Marine- HCC Cyber & Professional Lines Group
Reinsurance & Programs

Agenda

- About Tokio Marine HCC
- Cyber Landscape
- What is Ransomware?
- Why is Ransomware Harmful?
- Best Practices to Avoid a Ransomware Attack
- Q&A





About Tokio Marine HCC



Tokio Marine HCC

Part of Tokio Marine, a premier global company

FOUNDED IN

1879

MARKET CAP

33 billion*

Underwrites over

100 CLASSES

of specialty insurance

Over

18 DIFFERENT BUSINESS UNITS

Highly rated insurance
company achieving



**A.M.
Best**

SUPERIOR



**S&P Global
Ratings**

STRONG



**Fitch
Ratings**

VERY STRONG

*Figures as of 03/31/2021

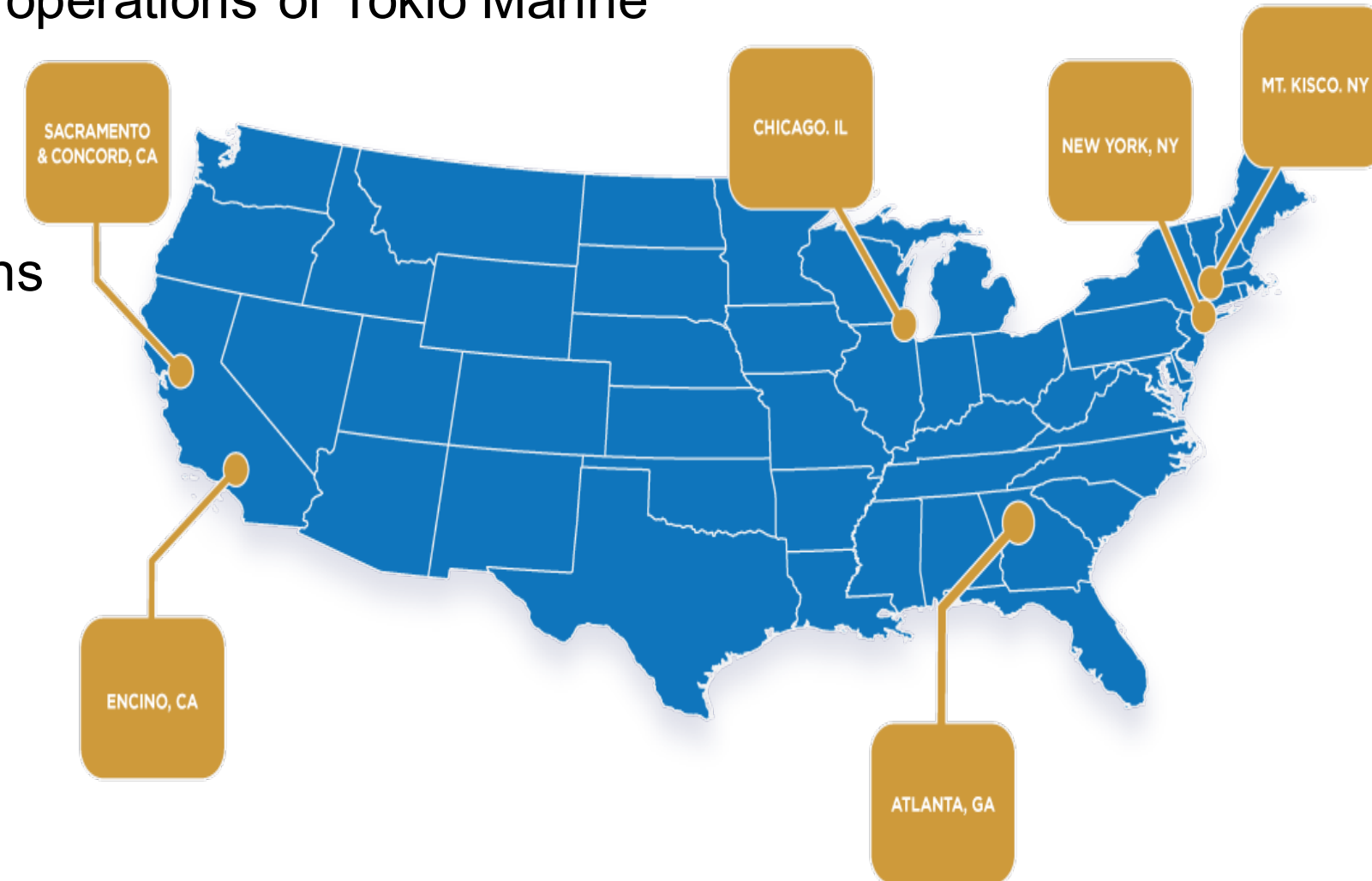
Company confidential – Not for distribution

Tokio Marine HCC – Cyber & Professional Lines Group



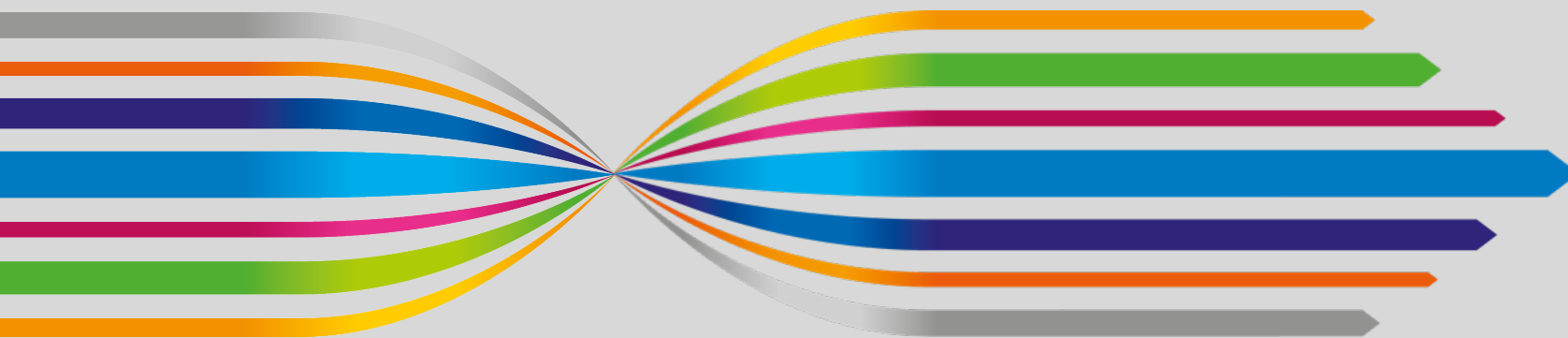
Tokio Marine HCC – CPLG is the marketing name used to describe the cyber and professional lines related insurance operations of Tokio Marine HCC

- Formed in April 2019
- Provides unique specialty insurance solutions
- Product lines include:
 - Tech & Cyber
 - Professional Liability
 - Reinsurance & Programs



Over \$150 million in Annual Cyber Premium

Over 2,200 cyber matters handled per year



Cyber Landscape

Ripped from the Headlines

Ryuk ransomware responsible
for one third of all ransomware
attacks in 2020

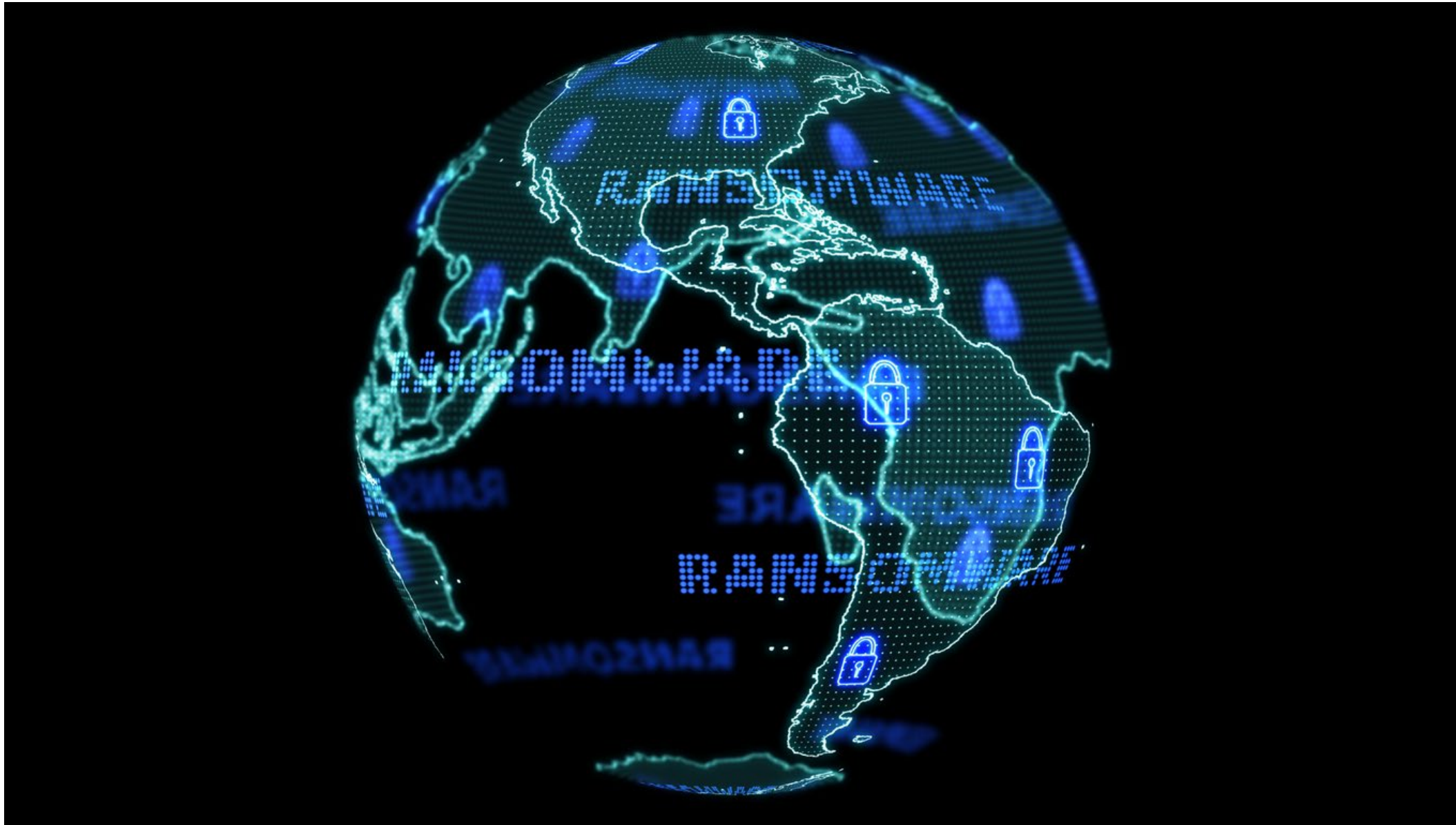
Blackbaud ransomware attack
may have impacted millions
of individuals

WannaCry: Massive ransomware
infection hits computers
in 99 countries

Hackers breached Colonial Pipeline
using compromised password

'Payment sent'- travel giant
CWT pays \$4.5M ransom to
cyber criminals

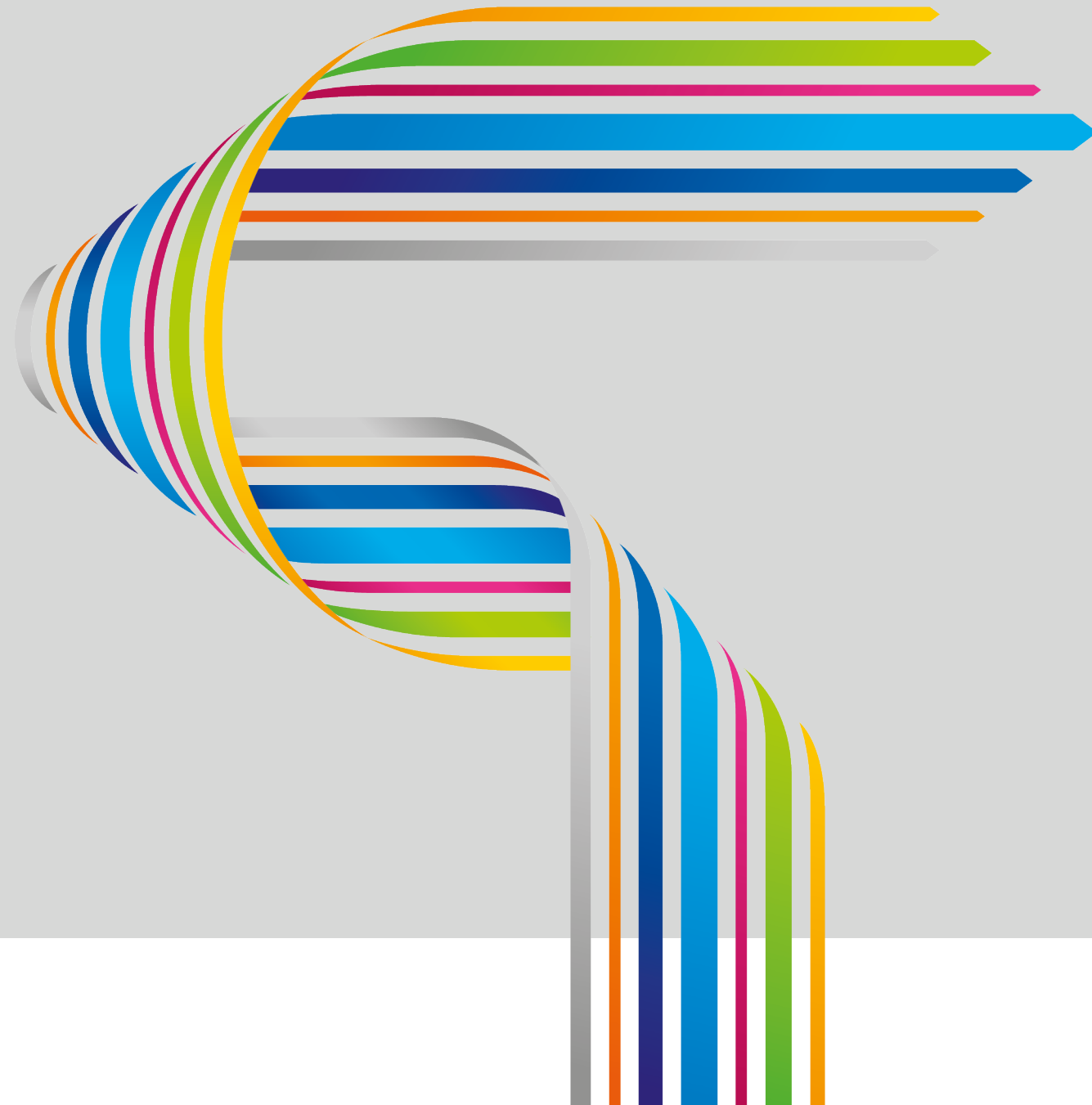
Ransomware- Global Impact



Catholic Mutual Ransomware Claims Statistics



Contract Year	7/1/2018	7/1/2019	7/1/2020	2021 (YTD)	Total
Ransomware Claims	5	13	16	1	35
Closed	5	13	7	0	25
Open	0	0	9	1	10
Total Paid	\$162,965	\$1,000,484	\$922,774	\$16,151	\$2,103,374
Average Paid	\$32,593	\$76,960	\$57,673	\$16,151	\$60,068



What is Ransomware?

Ransomware is a malware that locks your organization's data and prevents you from accessing it until you pay a ransom.



Ransomware Scenario

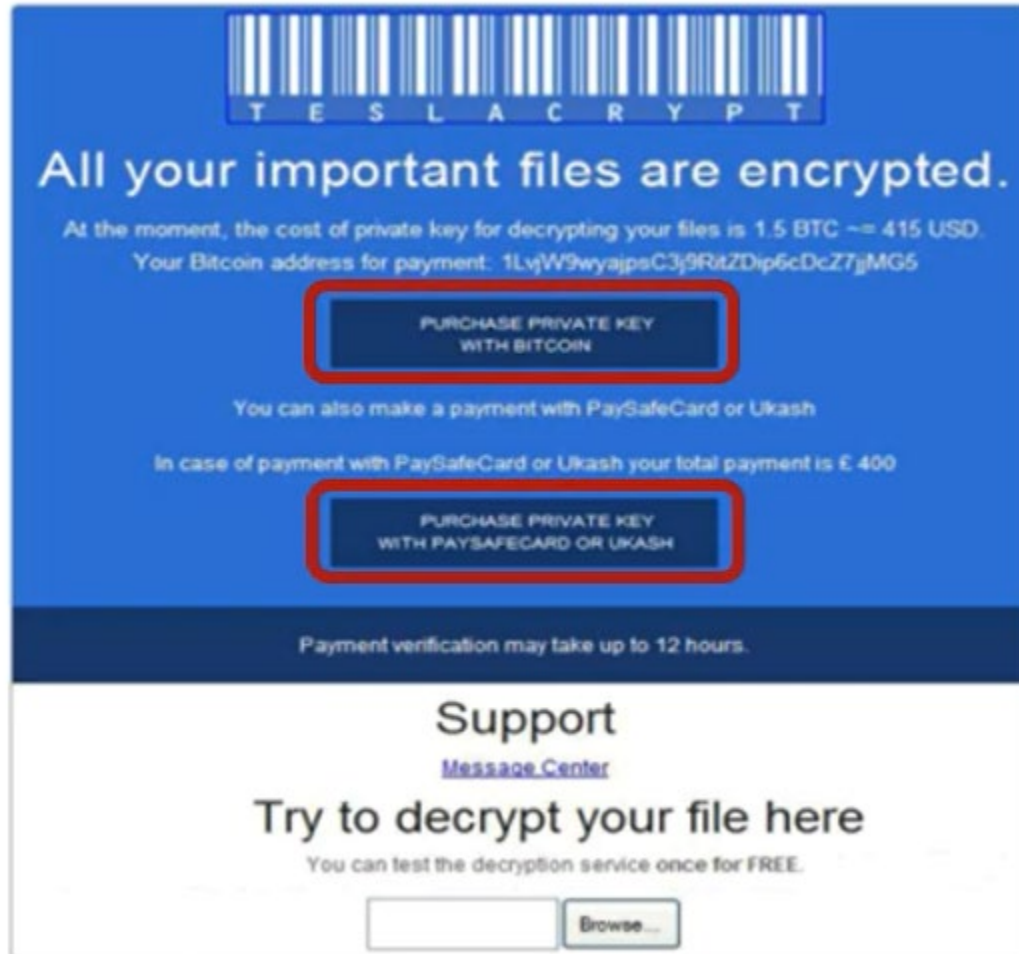


An employee opened a link in an email, that appeared to be sent by another employee of the firm, but it was actually sent by a hacker.

The link contained a ransomware virus that, when opened, immediately began to encrypt all files on the employee's computer, including the finance and payroll files.

The virus was discovered when the employee tried to access a file, and an alert appeared on the screen, notifying that all files had been encrypted and could only be unlocked if a 'ransom' was paid in BitCoin.

Examples of Ransomware messages



TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~ 415 USD.
Your Bitcoin address for payment: 1LvW9wyaipsC3j9RitZDip6cDcZ7jMG5

**PURCHASE PRIVATE KEY
WITH BITCOIN**

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is € 400

**PURCHASE PRIVATE KEY
WITH PAYSAFECARD OR UKASH**

Payment verification may take up to 12 hours.

Support
[Message Center](#)

Try to decrypt your file here
You can test the decryption service once for FREE.



WARNING

We have encrypt your files with CryptoLocker virus

 Your important files (including those on the network disk(s), USB, etc): photos, videos, documents etc. were encrypted with CryptoLocker virus. The only way to get your files back is to buy our decryption software.

Caution: Removing of CryptoLocker will not restore access to your encrypted files. The only way to save your files is to buy a decryption software. Otherwise, your files will be lost.

[Click here to buy decryption software](#)

Our website should also be accessible from one of these links:

- <http://erhltnefvgajflw.tor2u.net/buy.php?71.mnd>
- <http://erhltnefvgajflw.doe2tor.org/buy.php?71.mnd>
- <http://erhltnefvgajflw.tor2web.org/buy.php?71.mnd>
- <http://erhltnefvgajflw.onion.sah/buy.php?71.mnd>

Frequently Asked Questions

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files ?

All of your files were protected by a strong encryption with RSA4096

More information about the encryption keys using RSA4096 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

How did this happen ?

!!! Specially for your PC was generated personal RSA4096 Key , both public and private.

!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.

!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?

So , there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BITCOIN NOW! , and restore your data easy way

If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment

Your personal ID: **861782E3D50E**

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- 1 - <http://hn5fbbc4pyz77xfa.onion.to>
- 2 - <http://hn5fbbc4pyz77xfa.onion.cab>
- 3 - <http://hn5fbbc4pyz77xfa.onion.city>

If for some reasons the addresses are not available, follow these steps:

- 1 - Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- 2 - After a successful installation, run the browser
- 3 - Type in the address bar - <http://hn5fbbc4pyz77xfa.onion>
- 4 - Follow the instructions on the site

Be sure to copy your personal ID and the instruction link to your notepad not to lose them.

OFAC Advisory on Ransomware

- **October 2020:** The Office of Foreign Assets Control (OFAC) issued an advisory of sanctions risks associated with ransomware payments, related to malicious cyber-enable activities. OFAC has designated numerous malicious cyber actors, under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions.
- **September 2021:** OFAC issues an updated advisory OFAC urging companies that engage with victims of ransomware attacks (i.e., cyber insurers, digital forensics and incident response firms and financial institutions) to implement sanctions compliance programs that account for the risk that a ransomware payment may involve a Specially Designated Nationals and Blocked Persons List (“SDN List”).

TMHCC claims team always has OFAC clearance before approving ransom reimbursements.



Why is Ransomware Harmful?

Why is Ransomware Harmful?

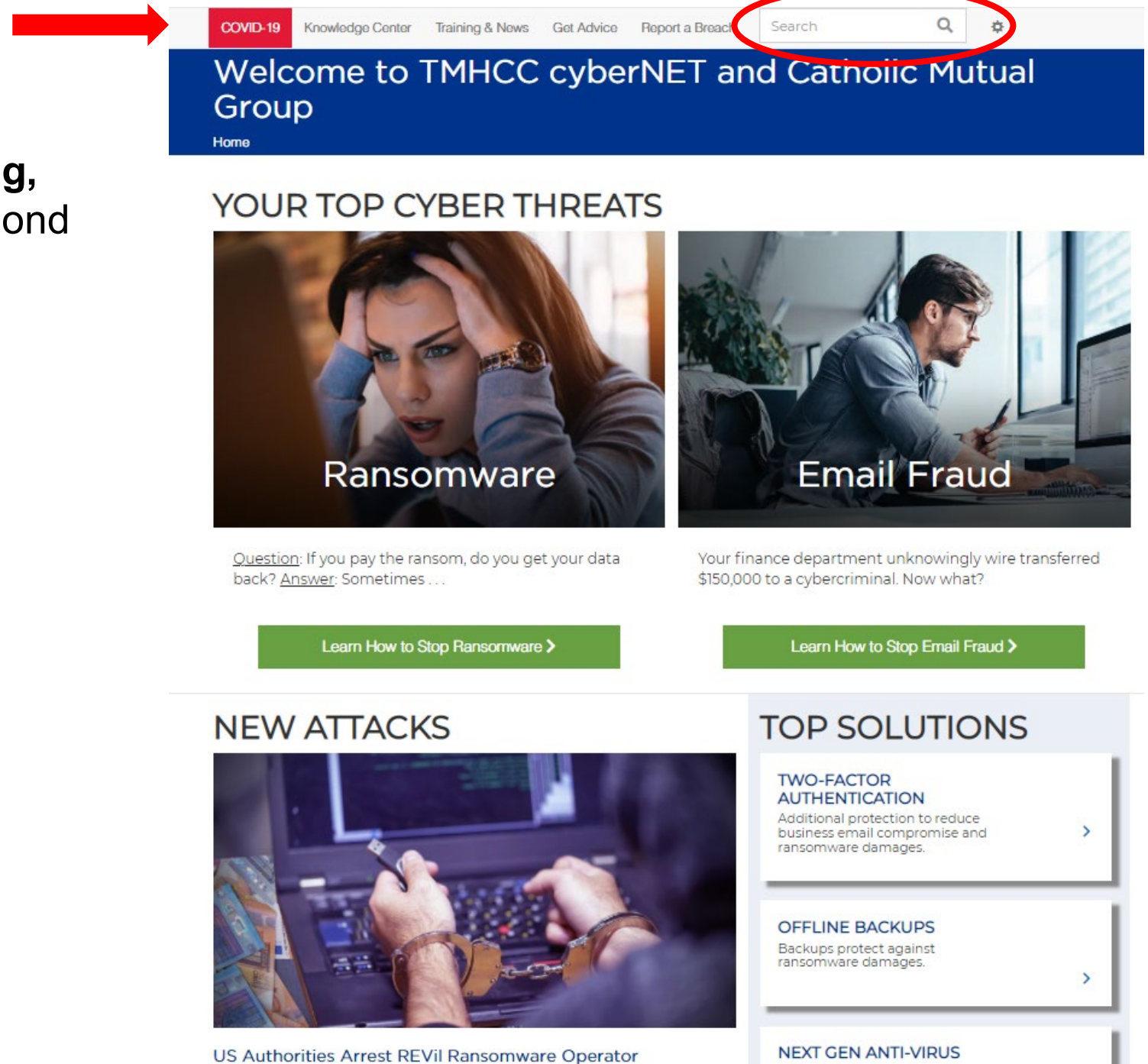
- Information is extremely valuable as organizations cannot function without access to their files.
- Ransomware is low risk for criminals, as they request their ransom to be paid in Bitcoin, so they remain completely anonymous.
- Once downloaded into a victim's computer, it can spread to all connected devices.
- Ransomware is used to steal data and/or move laterally within a corporate network to perform reconnaissance.
- All organizations are potential victims and might have to pay the ransom to regain access to their data.



Risk Management

CYBER RISK MANAGEMENT

- 24/7 access to CyberNET risk management website provides your Insureds with vital **information, training, and support** to prepare for, defend against, and respond to a cyber incident.
- Best Practices Guidelines
- Risk Assessments and Fitness Checklists
- Incident Response Planning
- Online Training Courses
- Sample Policies / Procedures



The screenshot shows the TMHCC cyberNET website. A red arrow points to the search bar in the top navigation bar. The website features a blue header with the text "Welcome to TMHCC cyberNET and Catholic Mutual Group" and a "Home" link. Below the header, there is a section titled "YOUR TOP CYBER THREATS" with two main cards: "Ransomware" and "Email Fraud". Each card includes a question, an answer, and a "Learn How to Stop" button. The "Ransomware" card shows a woman looking distressed, and the "Email Fraud" card shows a man working at a computer. Below these, there are two more sections: "NEW ATTACKS" featuring a card about the arrest of a REvil ransomware operator, and "TOP SOLUTIONS" featuring cards for "TWO-FACTOR AUTHENTICATION", "OFFLINE BACKUPS", and "NEXT GEN ANTI-VIRUS".

COVID-19 Knowledge Center Training & News Get Advice Report a Breach Search

Welcome to TMHCC cyberNET and Catholic Mutual Group
Home

YOUR TOP CYBER THREATS

Ransomware
Question: If you pay the ransom, do you get your data back? Answer: Sometimes...

[Learn How to Stop Ransomware >](#)

Email Fraud
Your finance department unknowingly wire transferred \$150,000 to a cybercriminal. Now what?

[Learn How to Stop Email Fraud >](#)

NEW ATTACKS

US Authorities Arrest REvil Ransomware Operator

TOP SOLUTIONS

TWO-FACTOR AUTHENTICATION
Additional protection to reduce business email compromise and ransomware damages.

OFFLINE BACKUPS
Backups protect against ransomware damages.

NEXT GEN ANTI-VIRUS

Top 8 Ways to Beat Ransomware

1. Train Employees
2. RDP & Access Control
3. Install Software Patches
4. Create Offline Backups
5. Implement Multi-factor Authentication (MFA)
6. Install & Update “Next-Gent” Antivirus
7. Email Security Settings
8. Endpoint Security



Claims Handling

Claims Handling



- Just like a normal claim, Members report claims directly to Catholic Mutual.
- Claims are forwarded to TMHCC
- Single Point of Contact
- Logical Procedural Steps
- Consistent communication and coordination with Catholic Mutual and policyholders

Questions?

Thank You!

Susan Doucette
sdoucette@tmhcc.com



TOKIO MARINE

HCC

Learn more about Tokio Marine HCC:
www.tmhcc.com

DATA SOURCES by SLIDE – Cyber Liability Coverage



Ripped from the Headlines:

Colonial Pipeline- Bloomberg.com: <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>

Blackbaud-

Benefitspro.com- <https://www.benefitspro.com/2020/10/12/blackbaud-ransomware-attack-may-have-impacted-millions-of-individuals/?slreturn=20220011161218>

Identity Theft Resource Center- <https://www.idtheftcenter.org/post/blackbaud-data-breach-leaves-lasting-impact-on-u-s-and-international-nonprofits/>

CWT- Reuters.com- <https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W>

Ryuk- Securitymagazine.com- <https://www.securitymagazine.com/articles/93769-ryuk-ransomware-responsible-for-one-third-of-all-ransomware-attacks-in-2020>

Zdnet.com- <https://www.zdnet.com/article/ryuk-gang-estimated-to-have-made-more-than-150-million-from-ransomware-attacks/>

WannaCry- BBC News- <https://www.bbc.com/news/technology-39901382>

“White House Holds Global Ransomware Meeting”- posted on TMHCC cyberNET and Catholic Mutual Group risk management website October 18, 2021

Risk Scenario Slides

These risk/claim scenarios are provided here for illustrative purposes only. The scenarios are examples of the types of claims and associated costs commonly seen and do not represent a comprehensive explanation of any one particular claim. While the subject coverage is designed to address certain risks and associated costs, coverage may not be available in all circumstances. Each reported claim will be evaluated on a case-by-case basis. The actual policy or endorsement language should be referenced to determine coverage applicability and availability.

